UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JUAN ORLANDO HERNANDEZ,
a/k/a "JOH,"

Defendant.

S7 15 Cr. 379 (PKC)

and with the limited objections of defendant Juan Orlando Hernandez (ECF 540 & 540-1.)

PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION

This matter comes before the Court upon the Government's Motion for Protective Order Pursuant To Section 3 of the Classified Information Procedures Act ("CIPA"). Pursuant to the authority granted under Section 3 of CIPA, the "Revised Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information" (hereinafter "Security Procedures," which are reprinted after CIPA § 9), Rules 16 and 57 of the Federal Rules of Criminal Procedure, and the general supervisory powers of the Court, and to protect the national security, the following Protective Order is entered[1]:

1. The Court finds that this case will involve information that has been classified in the interest of national security. The storage, handling, and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to this information requires appropriate security clearances and need-to-know, as set forth in

[1] The Court understands that the Government may move for a supplemental protective order depending on the nature of additional information that is determined to be discoverable.

Executive Order 13256 (or successor order), that has been validated by the Government.[2] The purpose of this Order is to establish procedures that counsel and the parties must follow in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information and may be modified from time to time by further Order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

2. Definitions. The following definitions shall apply to this Order:

a. "Defense" or "defense team" refers collectively to the Defendant's counsel and any support staff, investigators, or experts assisting the Defendant's counsel authorized to receive classified information pursuant to this Order.

b. "Classified information" shall include:

i. Any document, recording, or information that has been classified by any Executive Branch agency in the interests of national security pursuant to Executive Order 13526, as amended, or its predecessor or successor orders, as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI");

ii. Any document, recording, or information now or formerly in the possession of a private party that (A) has been derived from information that was classified by the United States Government, and/or (B) has been classified by the United States Government as set forth above;

[2] Any individual to whom classified information is disclosed pursuant to this Order shall not disclose such information to another individual unless the U.S. agency that originated that information has validated that the proposed recipient possesses an appropriate security clearance and need to know.

iii. Verbal or other unwritten or unrecorded information known to the Defendant or the defense team that has been classified by the United States Government as set forth above;

iv. Any information, regardless of its origin, that the defense knows or reasonably should know contains classified information, including information acquired or conveyed orally;

v. Any document, recording, or information as to which the defense has been notified orally or in writing contains classified information; and

vi. Any document, recording, or information that is classified, as set forth in subparagraph (i), above, and that the Court or Government has approved for limited authorized disclosure to the Defendant pursuant to the restrictions set forth herein. All classified information that the Court or Government approves for limited authorized disclosure to the Defendant will contain an appropriate classification marking and will be marked "Provided to JUAN ORLANDO HERNANDEZ in *United States v. Juan Orlando Hernandez*, S7 15 Cr. 379 (PKC)."

c. "Document," "materials," and "information" shall include, but are not limited to:

i. all written, printed, visual, digital, electronic, or audible matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), as well as metadata;

ii. notes (handwritten, oral, or electronic); papers; letters;

correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings, or other communications; bulletins; teletypes; telecopies; telegrams; telexes; transcripts; cables; facsimiles; invoices; worksheets and drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes, disks, or thumb drives and all manner of electronic data-processing storage; and alterations, modifications, changes, and amendments of any kind to the foregoing; and

iii. information obtained orally.

d. "Access to classified information" shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

e. "Secure Area" shall mean a sensitive compartmented information facility ("SCIF") approved by a designated Classified Information Security Officer ("CISO") for the storage, handling, and control of classified information.

Classified Information

3. All classified documents, and classified information contained therein, shall remain classified unless the documents bear a clear indication that they are not classified or have been declassified by the agency or department that originated the document or information contained therein ("originating agency").

4. All access to classified information shall conform to this Order and the Memorandum of Understanding described herein.

5. Any classified information provided to the defense by the Government is to be used

solely by the defense and solely for the purpose of preparing the defense. The defense may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

6. The defense may not disclose classified information to the Defendant unless that same information has been previously disclosed to the defense by the Defendant or unless the Government has approved its release to the Defendant and marked it "Provided to JUAN ORLANDO HERNANDEZ in *United States v. Juan Orlando Hernandez*, S7 15 Cr. 379 (PKC)." The defense may not confirm or deny to the Defendant the assertions made by the Defendant based on knowledge the defense may have obtained from classified information, except where that classified information has been provided to the Defendant pursuant to this Order. Any classified information the defense discloses to or discusses with the Defendant in any way shall be handled in accordance with this Order and the attached Memorandum of Understanding, including such requirements as confining all discussions, documents, and materials to an accredited SCIF.

7. The defense and the Defendant shall not disclose classified information to any person, except to the Court, Government personnel who hold appropriate security clearances and have been determined to have a need to know that information, and those specifically authorized to access that information pursuant to this Order.

8. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who, by virtue of this Order or any other court order, are granted access to classified information may not confirm or deny classified information that appears in the public

domain. Prior to any attempt by the defense to have such information confirmed or denied at trial or in any public proceeding in this case, the defense must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

9. In the event that classified information enters the public domain, the defense is precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that the defense had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. If there is any question as to whether information is classified, the defense must handle that information as though it is classified unless Government counsel (or the CISO) confirms that it is not classified.

Security Procedures

10. In accordance with the provisions of CIPA and the Security Procedures, the Court has designated Matthew Mullery as the CISO for this case for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified information that has been made available to the defense in connection with this case. If Mr. Mullery is unavailable, Daniel O. Hartenstine, Daniella M. Medel, Connor B. Morse, Harry J. Rucker, and Winfield S. Slade will serve as alternate CISOs. The defense shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

11. The Government has advised the Court that Assistant United States Attorneys Jacob H. Gutwillig, David J. Robles, Elinor L. Tarlow, and Kyle A. Wirshba, as well as their supervisors ("Government counsel"), have the security clearances allowing them to have access to classified information that Government counsel intend to use, review, or disclose in this case.

12. The Court has been advised, through the CISO, that a member of the defense team, Sabrina Shroff, Esq., has been granted security clearances permitting her to have access to the classified information that Government counsel intend to use and disclose pursuant to this Order.

13. *Protection of Classified Information.* The Court finds that to protect the classified information involved in this case, to the extent that Sabrina Shroff, Esq., has the requisite security clearances and a "need to know" the classified information, she, and any other member of the defense team who subsequently receives the requisite security clearances and has a "need to know" the classified information, shall be given authorized access to classified national security documents and information as required by the Government's discovery obligations and subject to the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding attached hereto, and any other Orders of this Court.

14. The signed Memorandum of Understanding shall be filed with the Court, and executed copies of the Memorandum of Understanding shall be served upon the Government. The substitution, departure, or removal for any reason from this case of counsel for the Defendant or any other member of the defense, shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

15. Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, no court personnel required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first have received the necessary security clearance as determined by the CISO.

16. Any additional persons whose assistance the defense reasonably requires may have access to classified information in this case only if they are granted an appropriate security

clearance through the CISO, obtain approval from this Court with prior notice of the identity of the additional persons to the U.S. Government agency that originated the information, and satisfy the other requirements described in this Order for access to classified information.

17. An individual with a security clearance and a "need to know" as determined by any Government entity is not automatically authorized to disclose any classified information to any other individual, even if that other individual also has a security clearance. Rather, any individual who receives classified information may disclose that information only to an individual who has been determined by an appropriate Government entity to have both the required security clearance and a need to know the information.

18. *Secure Areas for the Defense.* The Court is informed that the CISO has arranged for approved Secure Areas for use by the defense. The CISO shall establish procedures to assure the Secure Areas are accessible during business hours to the defense, and at other times upon reasonable request as approved by the CISO in consultation with the United States Marshals Service. The Secure Areas contain a working area for the defense and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defense. The CISO, in consultation with counsel for the Defendant, shall establish procedures to assure that the Secure Areas are maintained and operated in the most efficient manner consistent with the protection of classified information and in compliance with accreditation requirements. No classified documents, material, recordings, or other information may be removed from the Secure Areas unless so authorized by the CISO. The CISO shall not reveal to the Government the content of any conversations they may hear among the defense, nor reveal the nature of the documents being reviewed, or the work being generated. The presence of

the CISO shall not operate to render inapplicable the attorney-client privilege.

19. *Filing of Papers by the Defense.* Any pleading or other document filed by the defense that the Defendant or counsel for the Defendant knows or reasonably should know contains classified information as defined in paragraph 2(a), shall be filed as follows:

a. The document shall be filed under seal with the CISO or an appropriately cleared designee and shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 5:00 p.m. Within a reasonable time after making a submission to the CISO, the defense shall file on the public record in the CM/ECF system a "Notice of Filing" notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall consult with representatives of the agency or agencies having the relevant classification authority in order to determine whether the pleading or document contains classified information. If the agency or agencies with classification authority determine that the pleading or document contains classified information, the CISO shall ensure the document is marked with the appropriate classification marking and remains under seal.

c. The CISO shall immediately deliver or, if required, arrange for delivery by an appropriately cleared designee under seal to the Court and Government counsel any pleading or document to be filed by the defense that contains classified information, unless the pleading or document is an ex parte filing.

20. *Filing of Papers by the Government.* Any pleading or other document filed by the

Government that Government counsel knows or reasonably should know contains classified information as defined in paragraph 2(a), shall be filed as follows:

a. The document shall be filed under seal with the CISO or an appropriately cleared designee and shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 5:00 p.m. Within a reasonable time after making a submission to the CISO, Government counsel shall file on the public record in the CM/ECF system a "Notice of Filing" notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall consult with representatives of the agency or agencies having the relevant classification authority in order to determine whether the pleading or document contains classified information. If the agency or agencies with classification authority determine that the pleading or document contains classified information, the CISO shall ensure the document is marked with the appropriate classification marking and remains under seal.

c. The CISO shall immediately deliver or, if required, arrange for delivery by an appropriately cleared designee under seal to the Court and defense counsel any pleading or document to be filed by the defense that contains classified information, unless the pleading or document is an ex parte filing.

21. *Record and Maintenance of Classified Filings.* The CISO shall maintain a separate sealed record for those materials that are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

22. *The Classified Information Procedures Act.* Procedures for public disclosure of classified information in this case shall be those established by CIPA. The defense shall comply with the requirements of CIPA Section 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the defense shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to Government counsel and until the Government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the Government to appeal any adverse determination under CIPA Section 7 has expired or any appeal under Section 7 by the Government is decided. Pretrial conferences involving classified information shall be conducted *in camera* in the interest of the national security, be attended only by persons granted access to classified information and a need to know, and the transcripts of such proceedings shall be maintained under seal.

23. *Access to Classified Information.* In the interest of the national security, representatives of the defense granted access to classified information shall have access to classified information only as follows:

a. All classified information produced by the Government to counsel for the Defendant in discovery or otherwise, and all classified information possessed, created or maintained by the defense, including notes and any other work product, shall be stored, maintained and used only in the Secure Areas established by the CISO, unless otherwise authorized by the CISO.

b. *Special procedures for audio recordings.* Any classified audio recordings that the Government discloses to the defense shall be maintained by the CISO in the Secure Areas.

Such recordings may be reviewed only on a stand-alone, non-networked computer or other device within the Secure Areas that does not have the capability to duplicate or transmit information. The defense must use headphones to review such recordings and the headphones must be wired and not have any wireless capability.

c. The defense shall have free access to the classified information made available to them in the Secure Areas established by the CISO and shall be allowed to take notes and prepare documents with respect to those materials.

d. No representative of the defense (including but not limited to counsel, investigators, paralegals, translators, experts, and witnesses) shall copy or reproduce any classified information in any manner or form, except with the approval of the CISO and in accordance with the procedures established by the CISO for the operation of the Secure Area.

e. All documents prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in the Secure Areas on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, thumb drives, discs, CDs, DVDs exhibits, and electronic or digital copies) that may contain classified information shall be maintained in the Secure Areas unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to Government counsel or any other party.

f. The defense shall discuss classified information only within the Secure Areas or in an area authorized by the CISO.

g. The defense shall not disclose, without prior approval of the Court, classified information to any person not named in this Order except to the Court, Court personnel, and Government personnel identified by the CISO as having the appropriate clearances and the need to know. Government counsel shall be given an opportunity to be heard in response to any defense request for disclosure to a person not identified in this Order. Any person approved by this Court for access to classified information under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to this Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, the Department of Justice (through the CISO) shall promptly seek to obtain security clearances for them at the request of defense counsel. As set forth above, the defense shall not disclose classified information, even to an individual with the appropriate security clearance, without following the procedure referenced in paragraph 16.

h. The defense shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the Internet and email, or in the presence of any person who has not been granted access to classified information by the Court.

i. Any documents written by the defense that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

j. The defense shall not disclose classified information to the Defendant—other than materials marked "Provided to JUAN ORLANDO HERNANDEZ in *United States v.*

Juan Orlando Hernandez, S7 15 Cr. 379 (PKC)"—absent written permission from the Government.

24. Any unauthorized disclosure or mishandling of classified information may constitute violations of federal criminal law. In addition, any violation of the terms of this Order shall be brought immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention, or handling of classified documents or information could cause serious damage, and in some cases exceptionally grave damage to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. The purpose of this Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it.

25. All classified documents and information to which the defense has access in this case are now and will remain the property of the United States. Upon demand of the CISO, all persons shall return to the CISO all classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information. The notes, summaries, and other documents prepared by the defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of the case. At the conclusion of this case, including any appeals or ancillary proceedings thereto, all such notes, summaries, and other documents are to be destroyed by the CISO in the presence of counsel for the Defendant if they choose to be present. Even upon the

conclusion of this case, the parties, counsel, and any of their representatives or associates to whom classified documents or information was disclosed, remain obligated to protect against the unauthorized disclosure of any classified information learned during the course of the proceedings, as described herein.

26. Nothing contained in this Order shall be construed as a waiver of any right of the Defendant. No admission made by the Defendant or his counsel during pretrial conferences may be used against the Defendant unless it is in writing and signed by the Defendant. *See* CIPA § 2.

27. Nothing in this Order shall be construed to require the defendant to disclose information protected by the attorney-client privilege or its work product to the government's trial team.

[INTENTIONALLY LEFT BLANK]

28. This Order is subject to modification by this Court by a written Order expressly referencing this Order.

27. A copy of this Order shall be issued forthwith to counsel for the Defendant who shall be responsible for advising the Defendant and representatives of the defense of the contents of this Order. Counsel for the Defendant, the Defendant, and any other representatives of the defense who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 14 of this Order, and the Defendant and counsel for the Defendant shall file executed originals of such documents with the Court and the CISO and serve an executed original upon the Government. The execution and filing of the Memorandum of Understanding is a condition precedent for the Defendant, counsel for the Defendant, and any other representative of the defense to have access to classified information.

Dated: April 4, 2023

SO ORDERED:

THE HONORABLE P. KEVIN CASTEL
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. - JUAN ORLANDO HERNANDEZ, a/k/a "JOH," Defendant.	S7 15 Cr. 379 (PKC)

MEMORANDUM OF UNDERSTANDING REGARDING RECEIPT OF CLASSIFIED INFORMATION

Having familiarized myself with the applicable statutes, regulations, and orders, including but not limited to, Title 18, United States Code, Sections 793, 794, 798, and 1924; the Intelligence Identities Protection Act, Title 50, United States Code, Section 3121; Title 18, United States Code, Section 641; Title 50, United States Code, Section 783; and Executive Order 13526, I understand that I may be the recipient of information and documents that concern the present and future security of the United States and which belong to the United States, and that such documents and information together with the methods and sources of collecting it are classified by the United States Government. In consideration for the disclosure of classified information and documents:

(1) I agree that I shall never divulge, publish, or reveal either by word, conduct or any other means, such classified documents and information unless specifically authorized in writing to do so by an authorized representative of the United States Government; or as expressly authorized by the Court pursuant to the Classified Information Procedures Act and the Protective Order entered in *United States v. Juan Orlando Hernandez*, S7 15 Cr. 379 (PKC).

(2) I agree that this Memorandum will remain forever binding on me.

(3) I have received, read, and understand the Protective Order entered by the United States District Court for the Southern District of New York on _____, 2023, in *United States v. Juan Orlando Hernandez*, S7 15 Cr. 379 (PKC), relating to classified information, and I agree to comply with the provisions thereof.

(4) I understand that any prior contractual obligations that may bind me to continue to protect classified information remain in full force and effect, and are not superseded by this Memorandum of Understanding. Additionally, I understand that this Memorandum of Understanding does not absolve me of any criminal or civil penalties that may otherwise be imposed upon me as a result of my unauthorized disclosure of classified information.

_____ _____

Counsel for the Defendant Date